QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ July 13, 2004

Multiple Microsoft Vulnerabilities: Windows, Internet Explorer, & Outlook Express

ADVISORY OVERVIEW

July 13, 2004 – Qualys™ Vulnerability R&D Lab has released new vulnerability signatures in the QualysGuard® Service to protect organizations against the new critical Microsoft® vulnerabilities that were announced earlier today. Customers can immediately audit their networks for these and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft released a series of patches today, ranging in severity from Critical to Moderate, which remediate numerous flaws recently discovered in the Windows Operating System, Outlook Express, IIS, and the Internet Explorer browser. These vulnerabilities could potentially allow an attacker to execute malicious code on a vulnerable host.

These new vulnerabilities include:

1. **MS04-022:** A remote code execution vulnerability (CAN-2004-0212) exists in the Windows Task Scheduler caused by an unchecked buffer that is responsible for handling application name validation which, if exploited, could permit a malicious user to compromise the vulnerable host and gain the full privileges of the logged in user. This vulnerability has a severity rating of critical. http://www.microsoft.com/technet/security/bulletin/MS04-022.mspx

2. **MS04-023:** Two HTML Help vulnerabilities (CAN-2003-1041 & CAN-2004-0201) exist in Windows 2000, 2003, and XP which, if exploited, could permit a malicious user to compromise the vulnerable host and gain the full privileges of the logged in user. These vulnerabilities have a severity rating of critical. http://www.microsoft.com/technet/security/bulletin/MS04-023.mspx

3. **MS04-019:** Post-SP2 Windows 2000 servers and workstations contain a Utility Manager vulnerability (CAN-2004-0213) which, if exploited, could permit a logged in user to escalate their privileges

and take complete control over the vulnerable system. This vulnerability has a severity rating of important.
http://www.microsoft.com/technet/security/bulletin/MS04-019.mspx

4. **MS04-020:** Windows NT and post-SP2 Windows 2000 servers and workstations contain a POSIX subsystem vulnerability (CAN-2004-0210) which, if exploited, could permit a logged in user to escalate their privileges and take complete control over the vulnerable system. This vulnerability has a severity rating of important.
http://www.microsoft.com/technet/security/bulletin/MS04-020.mspx

5. **MS04-021:** Windows NT systems running IIS 4.0 contain a buffer overrun vulnerability (CAN-2004-0205) which, if exploited, could permit a malicious user to take complete control over the vulnerable system. This vulnerability has a severity rating of important.
http://www.microsoft.com/technet/security/bulletin/MS04-021.mspx

6. **MS04-024:** All Windows systems through Windows 2003 contain a Windows Shell vulnerability (CAN-2004-0420) which, if exploited, could permit a logged in user to escalate their privileges and take complete control over the vulnerable system. This vulnerability has a severity rating of important.

   NOTE: Exploitation of this vulnerability requires user interaction, such as a user visiting a malicious website.

   http://www.microsoft.com/technet/security/bulletin/MS04-024.mspx

7. **MS04-018:** Outlook Express 5.5 and 6, when running on any version of Microsoft Windows, contains a Denial-of-Service (DoS) vulnerability (CAN-2004-0215). A malicious user could send a "specially crafted" email that would cause Outlook Express to fail. This vulnerability has a severity rating of moderate.
http://www.microsoft.com/technet/security/bulletin/MS04-018.mspx

HOW TO PROTECT YOUR NETWORK

Audits for these new Microsoft Critical Security vulnerabilities are already available in the QualysGuard vulnerability management platform. A default scan using authentication will detect these issues and is the recommended detection method.

In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- **"Microsoft Outlook Express Denial of Service (MS04-018)"**
  - Qualys ID: 90136
  - Windows login required

- **"Windows HTML Help Remote Code Execution (MS04-023)"**

    - Qualys ID: 90135
    - Windows login required

- **"Windows Task Scheduler Code Execution (MS04-022)"**
    - Qualys ID: 90134
    - Windows login optional

- **"Windows POSIX Local Privilege Elevation (MS04-020)"**
    - Qualys ID: 90133
    - Windows login required

- **"Windows Utility Manager Local Privilege Elevation (MS04-019)"**
    - Qualys ID: 90132
    - Windows login required

- **"Windows Shell Remote Code Execution (MS04-024)"**
    - Qualys ID: 90137
    - Windows login required

- **"Microsoft IIS 4.0 Redirection Remote Code Execution (MS04-021)"**
    - Qualys ID: 86663
    - Windows login optional

  Additionally, enable the "Windows Host Name" signature with Qualys ID 82044 if you want to report on vulnerable hosts by Windows (NetBIOS) machine name.

TECHNICAL SUPPORT

For more information, customers may contact Qualys Technical Support directly at support@qualys.com or by telephone toll free at:
US: 1 866.801.6161 | EMEA: 33 1 44.17.00.41 | UK: +44 1753 872102

ABOUT QUALYSGUARD

QualysGuard is an on-demand security audit service delivered over the web that enables organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, QualysGuard dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

Access for QualysGuard customers: https://qualysguard.qualys.com

Free trial of QualysGuard service:
http://www.qualys.com/forms/trials/qualysguard_trial/